UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/878,320	06/12/2001	Mark Crosbie	100012170-1	2125

7590 06/28/2005

IP Administration
Legal Department, M/S 35
HEWLETT-PACKARD COMPANY
P.O. Box 272400
Fort Collins, CO 80528-9599

EXAMINER	
PARTHASARATHY, PRAMILA	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 06/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/878,320	CROSBIE ET AL.	
	Examiner	Art Unit	
	Pramila Parthasarathy	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 April 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12 and 14-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12 and 14-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on April 13, 2005. Claims 1, 18, 21 and 22 have been amended. New Claims 23 – 26 have been added. Claims 1 – 12 and 14 – 26 are pending.

Terminal Disclaimer

2. The terminal disclaimer filed on April 13, 2005 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of 09/878,319 has been reviewed and is accepted. The terminal disclaimer has been recorded.

Response to Remarks/Arguments

Claim Objections

3. Claim 1 is objected to because of the following informalities: Claim 1 recites, "...wherein at least one of said at one last one correlator...". For examination purposes, "wherein at least one of said at one last one correlator" is read as "wherein at least one of said one correlator".

4. Claims 1 and 23 – 26 are objected to because of the following informalities:

Claims 1 and 23 – 26 recite, "ECS engine" but do not expand what ECS represents. For examination purposes "ECS" is read as "Event Correlation Services".

Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1 – 12, 14 – 18 and 21 – 26 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

6. Claims 1 and 21 recites the limitation "event driven correlation" in the body of the claim language. There is insufficient antecedent basis for this limitation in the claim.

For examination purpose, "event driven correlation" will be read as "an event driven correlation".

7. Claim 23 recites the limitation "event correlation" in the body of the claim language. There is insufficient antecedent basis for this limitation in the claim.

For examination purpose, "event correlation" will be read as "an event driven correlation".

8. Claims 1 – 22 were rejected under 35 USC 102(e) as being anticipated by Moran (U.S. Patent Number 6,647,400, hereafter "Moran") and in response, Applicant amended Claims 1 and 21. Applicant has not explicitly or implicitly refuted the rejections for Claims 19 and 20 (See Remarks Page 7). Examiner correctly notes that Applicant is agreeing with the prior art disclosure and further states that the rejection for Claims 19 and 20 are maintained.

9. Applicant's remarks/arguments filed on April 13, 2005, with respect to amended Claims 1 and 21, have been fully considered but they are not persuasive. Referring to the previous Office action, Examiner had cited relevant portions of the references as a means to illustrate the system as taught by the prior art. As a means of providing further clarification as to what is taught by the references used in the first office action, Examiner has expanded the teachings for comprehensibility while maintaining the same grounds of rejection of the claims.

Moran teaches an intrusion detection system comprising an analysis engine and a configuration discovery mechanism for locating files, matching contents, signature checking mechanisms and also an event database of commands and files accessed by the commands, and a buffer overflow attack detector. The system is capable of handling

events that are seconds, days, weeks or longer ago and also provide an alert depending on the event.

10. Regarding amended independent Claims 1 and 21, Applicant agrees that Moran in a data driven but argues that the distinction between the prior art and the instant application is that the present invention "at least one of said at least one correlator uses event driven correlation services having an ECS (Event Correlation Services) engine core" and "using event driven correlation". These arguments are not persuasive.

Instant application discloses, "Event Correlation Services allows for the correlation of discrete events over time and ECS engine is embedded within the IDS correlator, to parse and understand kernel audit records, system log files and other data sources." (US2002/0083343 Page 7 paragraph [0136 – 0143]).

Moran discloses an intrusion detection system a mechanism (event correlation service) for checking discrete events and correlates them and assign a value to record associated with an event. Furthermore, Moran discloses scanning log files to form multiple correlations between dates for significant events (using event driven correlation), see Moran Column 4 lines 25 – 36 and Column 11 lines 15 – 54.

11. Applicant clearly has failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts. Therefore, the examiner

respectfully asserts that cited prior art does teach or suggest the subject matter broadly recited in independent claims 1 and 21. Dependent claims 2 – 12, 14 - 18 and 22 – 26 are also rejected at least by virtue of their dependency on independent claims and by other reason set forth in this office action.

Accordingly, the rejection for the pending Claims 1 – 12 and 14 – 26 is respectfully maintained.

Claim Rejections - 35 USC § 102

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

12. Claims 1 – 12 and 14 – 26 are rejected under 35 U.S.C. 102(e) as being anticipated by Moran (U.S. Patent Number 6,647,400).

Regarding Claim 1, Moran teaches and describes a computer architecture for an intrusion detection system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), comprising:

a control agent to interface with a management system and to monitor system activity (Column 5 line 26 – Column 6 line 51 and Column 8 lines 6 – 46);

at least one data gathering component which gathers kernel audit data and syslog data (Column 8 lines 6 – 46 and Column 10 lines 14 – 49);

at least one correlator to interpret and analyzes the kernel audit data and the syslog data using at least one detection template (Column 10 lines 14 – 49 and Column 11 lines 16 – 40),

wherein at least one of said one correlator uses event driven correlation services having an ECS engine core (Column 4 lines 25 – 36 and Column 11 lines 15 – 54).

Regarding Claim 19, Moran teaches and describes a computer architecture for an intrusions (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), comprising:

reading means for reading kernel records (Column 7 line 39 – Column 8 line 20 and Column 11 lines 15 – 54);

reformatting means for reformatting each of the read kernel records into a different format (Column 9 line 54 – Column 10 line 32);

parsing means for parsing the records and comparing the parsed records against one or more templates (Column 18 lines 6 – 58).

Regarding Claim 21, Moran teaches and describes a computer system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), comprising:

a processor (Column 5 line 26 – Column 6 line 51 and Column 8 lines 6 – 46); and

a memory coupled to said processor, the memory having stored therein sequences of instructions (Column 5 line 26 – Column 6 line 51 and Column 8 lines 6 –

46), which, when executed by said processor, causes said processor to perform the steps of:

reading kernel records (Column 7 line 39 – Column 8 line 20 and Column 11 lines 15 – 54);

reformatting each of the read kernel records into a different format (Column 9 line 54 – Column 10 line 32);

parsing the records and comparing the parsed records against one or more templates using event driven correlation (Column 4 lines 25 – 36, Column 11 lines 15 – 54 and Column 18 lines 6 – 58).

Claim 2 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein said intrusion detection system is host-based (Column 7 line 17 – Column 8 line 67).

Claim 3 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein said detection templates are configured into surveillance groups and into surveillance schedules (Column 23 lines 14 – 52; Column 35 lines 9 – 63 and Column 39 line 5 – Column 40 line 12).

Claim 4 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein said management system includes a graphical user interface (Column 8 lines 6 – 23).

Claim 6 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein there is low bandwidth connection between said control agent and each of said data gathering components and said at least one correlator and a high bandwidth connection between said control agent and each said data gathering component and said correlator (Column 11 lines 16 – 28 and Column 16 lines 40 – 45).

Claim 7 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein said correlator uses a meta-description language (Column 14 line 12 – Column 16 line 25).

Claim 8 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein said high bandwidth connection is used to send and receive memory mapped files

(Column 9 line 54 – Column 10 line 32; Column 11 lines 16 – 28 and Column 22 line 65 – Column 23 line 3).

Claim 9 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein said data gathering component includes a kernel audit record component and a syslog component (Column 8 line 6 – 46; Column 9 lines 12 – 65 and Column 10 lines 14 – 55).

Claim 11 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), further comprising a notification log and a response script connected to said control agent (Column 40 lines 13 – 37).

Claim 12 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), further comprising an installed bits file connected to said control agent (Column 8 lines 6 – 46 and Column 10 lines 14 – 49).

Claim 14 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the management system controls more than one control agent each residing on a different computer (Column 18 lines 6 – 58 and Column 31 lines 31 – 40).

Claim 15 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein said at least one template is selected from the group including:

reading kernel records (Column 7 line 39 – Column 8 line 20 and Column 11 lines 15 – 54);

reformatting each of the read kernel records into a different format (Column 9 line 54 – Column 10 line 32);

parsing the records and comparing the parsed records against one or more templates (Column 18 lines 6 – 58).

Claim 16 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein said control agent communicates with said management system across a secure communications link (Column 8 lines 6 – 46).

Claim 17 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein if the correlator detects an intrusion an alert will be sent to the management system and a potential intrusion alert record will be logged to a notification file (Column 8 line 6 – Column 9 line 32 and Column 40 lines 13 – 37).

Claim 18 is rejected as applied above in rejecting Claim 1. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein said at least one data gathering component includes a buffer (Column 8 lines 16 – 46 and Column 11 line 16 – Column 12 line 17).

Claims 20 and 22 are rejected as applied above in rejecting Claims 19 and 21. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein the one or more templates is chosen from the group including:

a modification of files/directories template (Column 18 lines 6 – 58 and Column 31 lines 31 – 40);

a change to log files template (Column 2 lines 40 – 47; Column 10 lines 14 – 55 and Column 11 lines 41 – 54);

a SetUID files template (Column 9 lines 33 – 47 and Column 12 lines 46 – 67);

a creation of world-writables template (Column 11 line 55 – Column 12 line 67);

a repeated failed logins template (Column 19 line 49 – Column 20 line 67);

a repeated failed SU commands template (Column 23 lines 14 – 46 and Column 25 lines 15 – 45);

a race conditions attack template (Column 12 lines 31 – 67);

a buffer overflow attacks template (Column 9 lines 33 – 47 and Column 33 line 64 – Column 34 line 42);

a modification of another user's file template (Column 18 lines 6 – 58 and Column 31 lines 31 – 40);

a monitor for the start of interactive sessions template (Column 38 lines 31 – 51); and

a monitor logins/logouts template (Column 23 lines 14 – 46 and Column 24 lines 33 – 41).

Claim 5 is rejected as applied above in rejecting Claim 4. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), further comprising a communication agent which encrypts information sent from said intrusion detection system to said management station (Column 16 lines 15 – 29).

Claim 10 is rejected as applied above in rejecting Claim 9. Furthermore, Moran teaches and describes a method of detecting intrusions using a host-based intrusion system (Fig. 2 – 4, 6; Summary and Column 5 line 10 – Column 38 line 25), wherein

said data gathering component and said syslog component convert gathered data into an ASCII format (Column 9 line 54 – Column 10 line 53; Column 11 lines 29 – 40 and Column 13 lines 26 – 31).

Claim 23 is rejected as applied above in rejecting Claim 22. Furthermore, Moran teaches wherein said event driven correlation has an ECS engine core (Column 4 lines 25 – 36 and Column 11 lines 15 – 54).

Claim 24 is rejected as applied above in rejecting Claim 22. Furthermore, Moran teaches wherein said ECS engine core uses a metadata language (Column 4 lines 25 – 36, Column 11 lines 15 – 54 and Column 17 line 50 – Column 18 line 5).

Claim 25 is rejected as applied above in rejecting Claim 24. Furthermore, Moran teaches wherein a translator module converts audit records and other events into internal ECS event format structure (Column 9 lines 12 – 47, Column 11 lines 15 – 54 and Column 13 lines 12 – 25).

Claim 26 is rejected as applied above in rejecting Claim 23. Furthermore, Moran teaches wherein said ECS engine core operates using an event driven model (Column 4 lines 25 – 36 and Column 11 lines 15 – 54).

Conclusion

13. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

14. Examiner's Note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

15. Applicant is urged to consider the references. However, the references should be evaluated by what they suggest to one versed in the art, rather than by their specific disclosure. If applicants are aware of any better prior art than those are cited, they are required to bring the prior art to the attention of the examiner.

16. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m.. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy
June 16, 2005.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100